iOS流量分析探索

陈作君

ABOUT ME

- 陈作君
- 🍊厂老司机客服

AGENDA

- 概览
- NE介绍
- 基于NE的流量分析

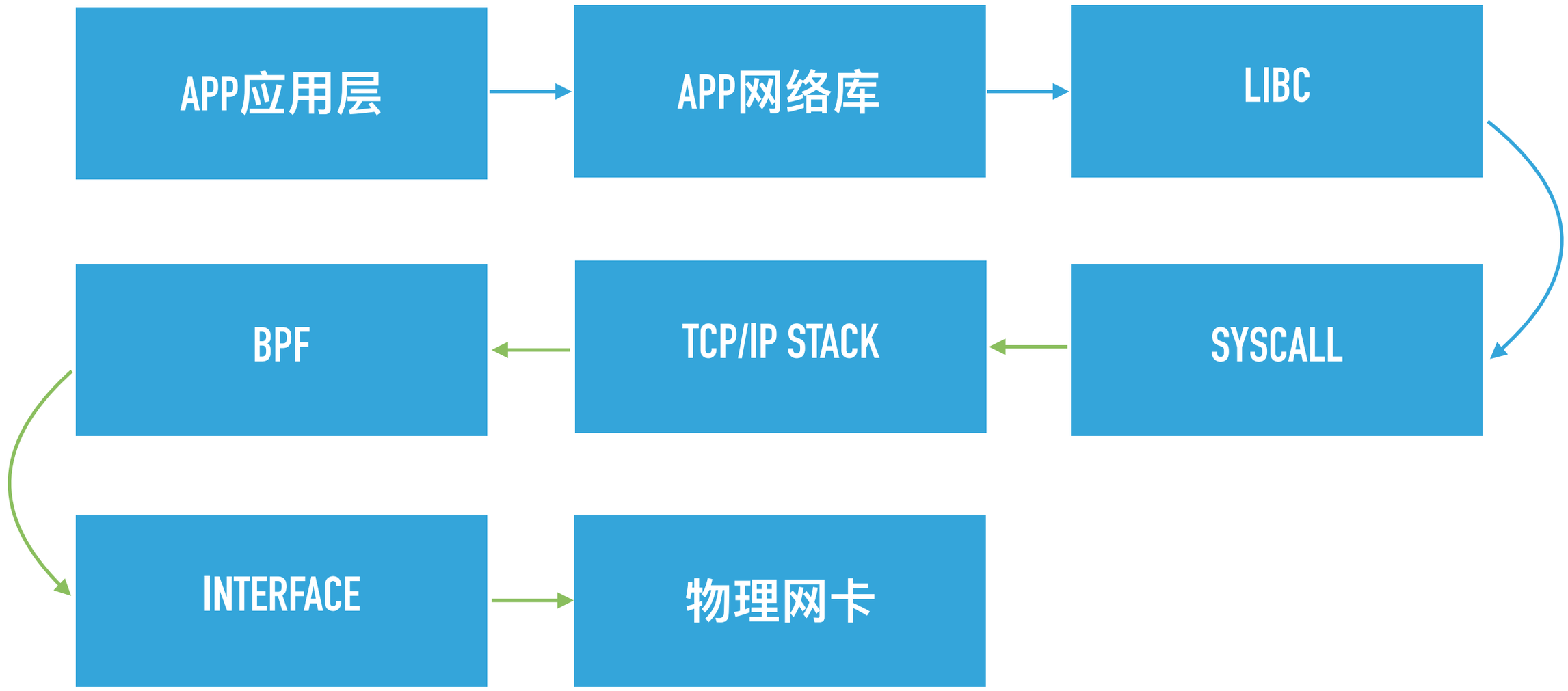
司机客服的自我修养

- “你能告诉我，流量都花到哪去了吗？”

起始时间	时长	总流量(KB)	通信费
12-01 07:00:00	48分24秒	1217	0.00
12-01 11:01:05	40分02秒	1	0.00
12-01 17:22:55	30分49秒	678	0.00
12-01 17:56:23	40分03秒	2065	0.00
12-01 18:36:36	10分00秒	355	0.00
2-01 18:46:39	40分03秒	2168	0.00
2-01 19:26:42	62分24秒	6967	0.00
2-01 20:29:06	40分07秒	1807	0.00
-01 21:09:13	63分42秒	3618	0.00
-01 22:12:55	80分05秒	2321	0.00
-01 23:33:00	40分00秒	1416	0.00
-02 00:13:00	40分00秒	2973	0.00
02 01:13:00	10分00秒	391	0.00
02 01:23:03	27分49秒	1040	0.00
02 01:52:00	37分41秒	2373	0.00

LET'S HOOK

一个请求的旅程



APP应用层

- NSURLProtocol
- 无法拦截CFNetwork层以下构造的请求
- 美团外卖移动端性能监控-Hertz

APP网络库

- NSURLSession/NSURLConnection
- CFNetwork
- 阿里百川/网易NeteaseAPM...

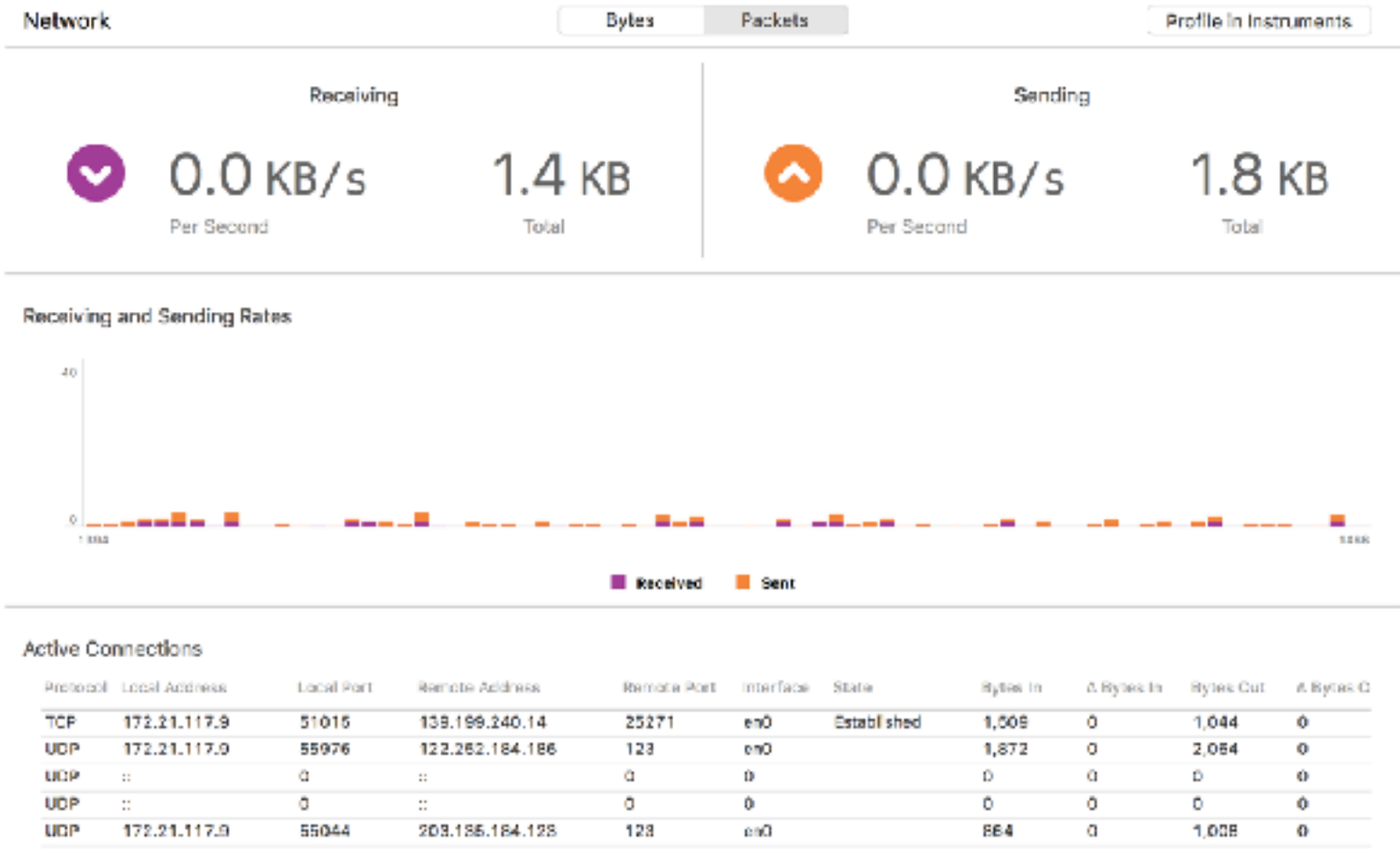
LIBC

- BSD Socket
- ProxyChains for iOS
- inline hook

```
#define hook(handle) ({ \
    _hook(handle, connect); \
    _hook(handle, sendto); \
    _hook(handle, gethostbyname); \
    _hook(handle, getaddrinfo); \
    _hook(handle, freeaddrinfo); \
    _hook(handle, gethostbyaddr); \
    _hook(handle, getnameinfo); \
    _hook(handle, close); \
})
    hook(RTLD_DEFAULT);
```

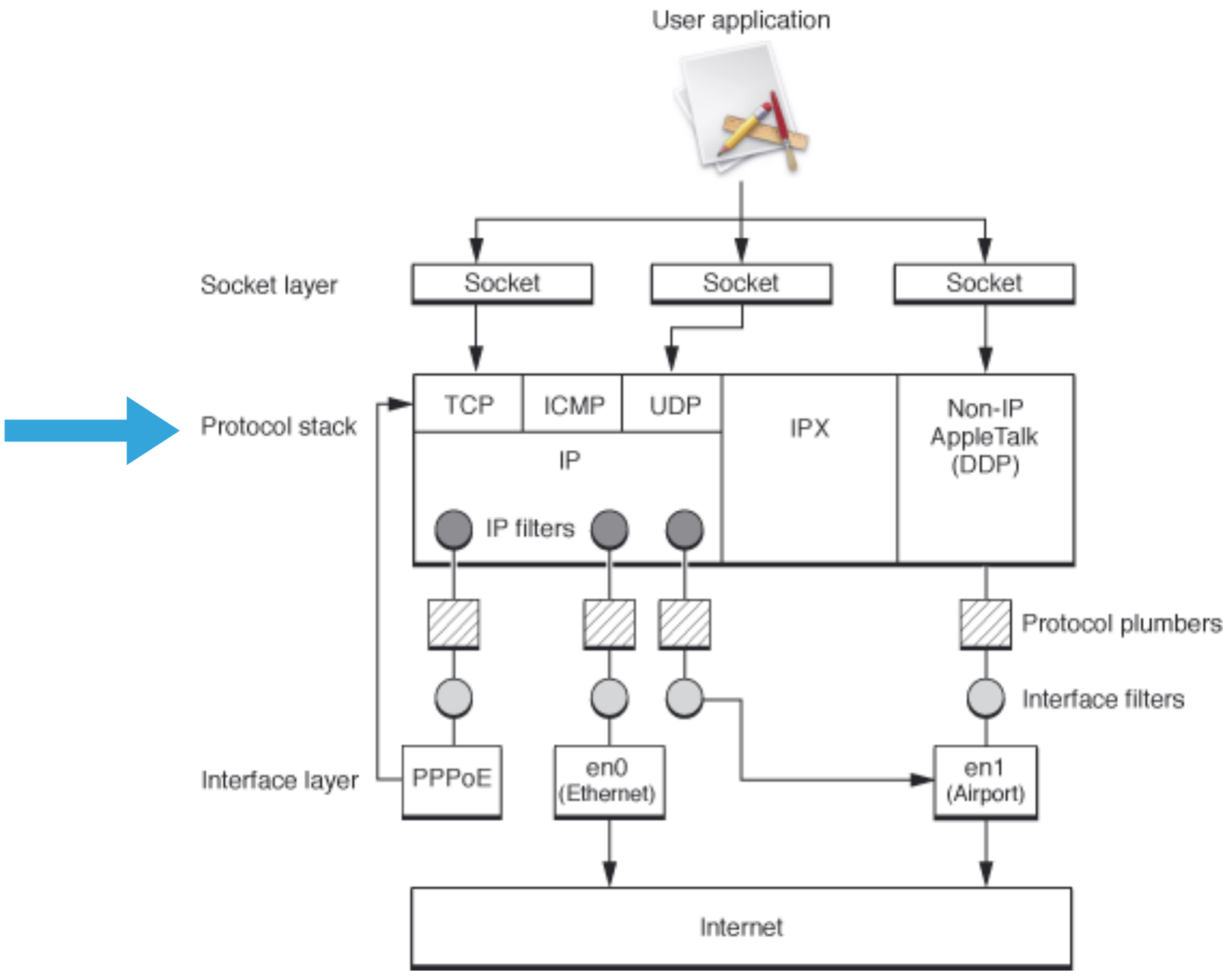
SYSCALL

- ptrace
- Xcode Instrument



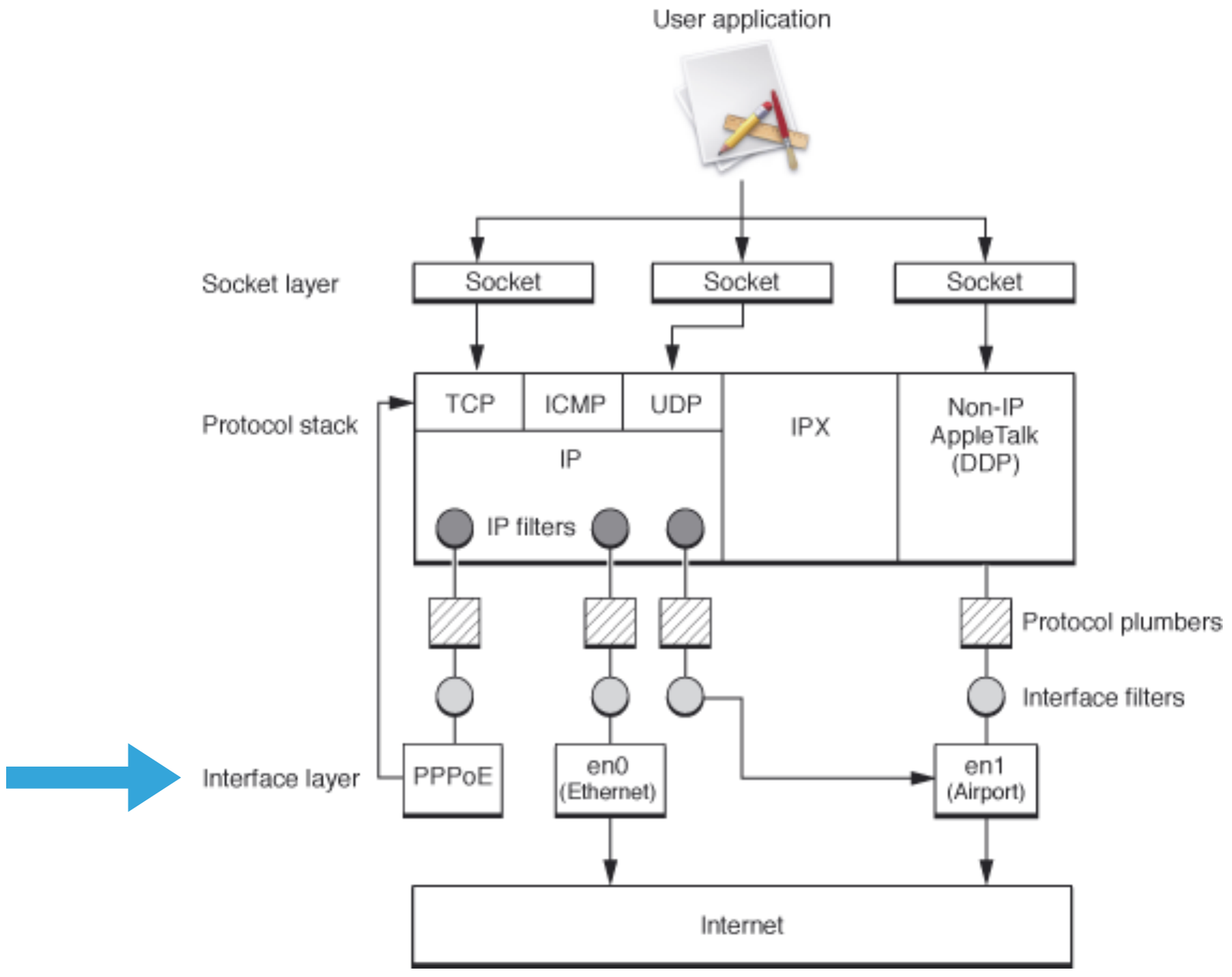
TCP/IP STACK

- IP Filters
- RootKit



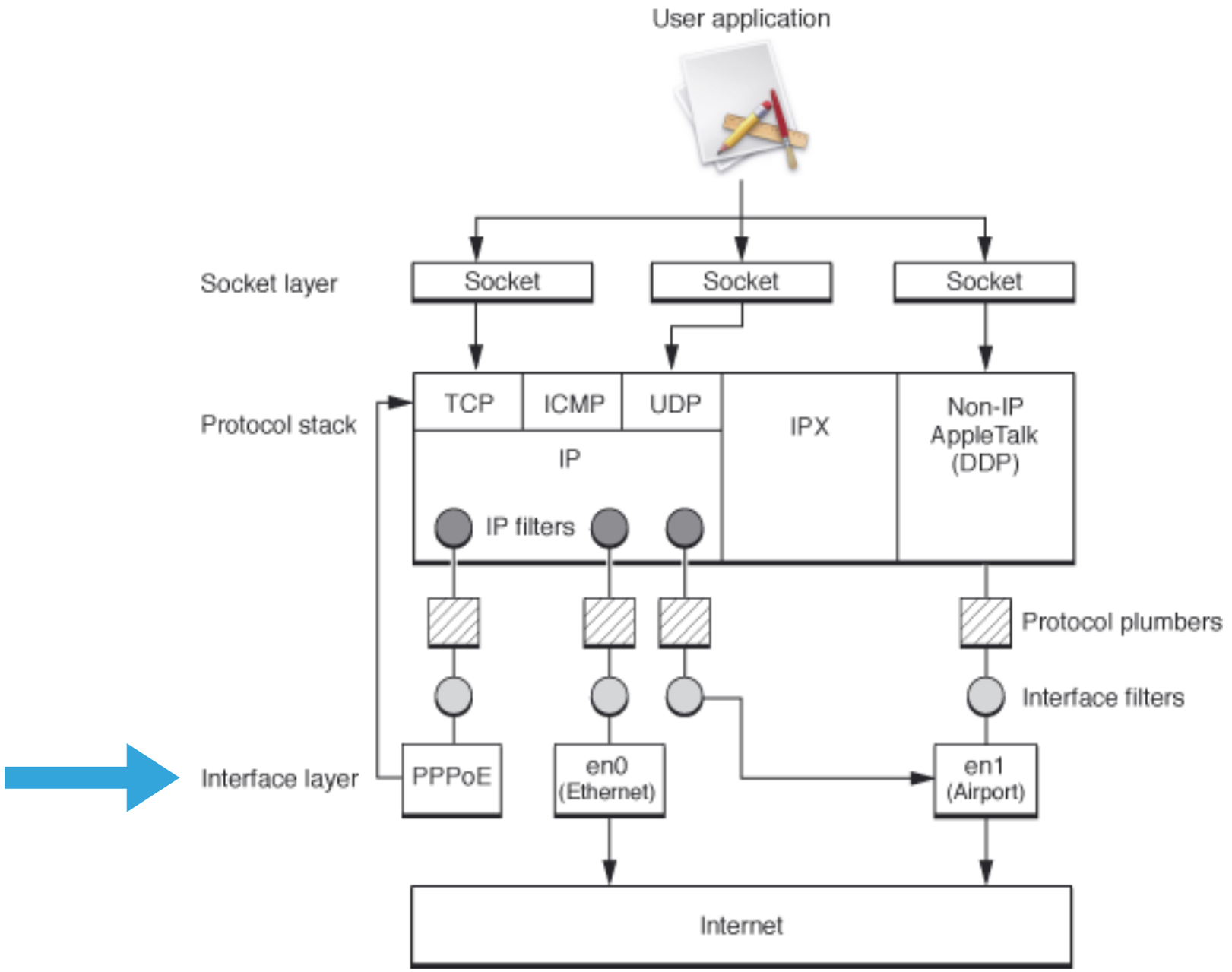
BPF

- TCPDUMP
- LIBPCAB



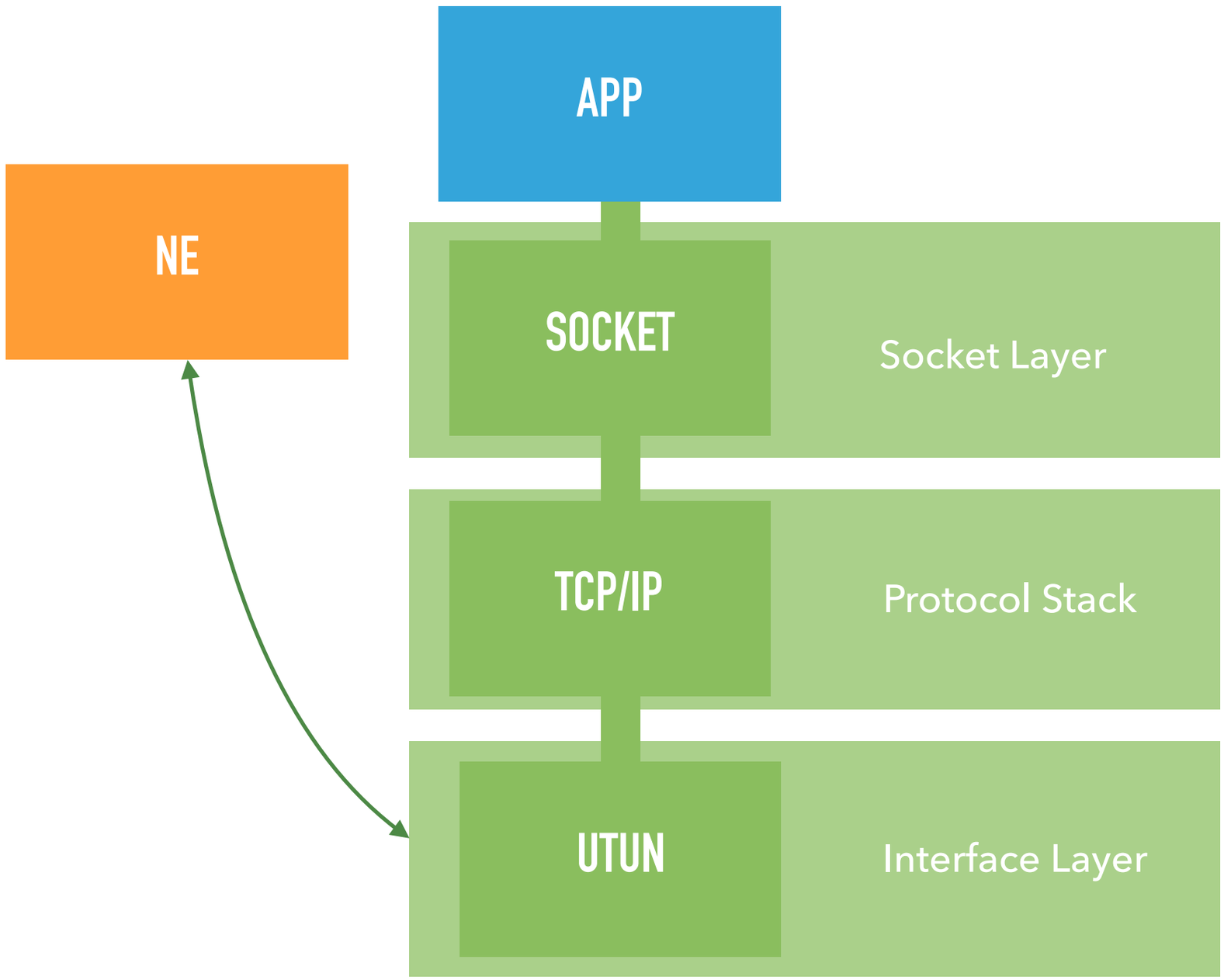
INTERFACE

- EN
- PDP
- 腾讯GT



UTUN

- Network Extension



AGENDA

- 概览
- NE介绍
- 基于NE的流量分析

WWDC 2015

WHAT'S NEW IN NETWORK EXTENSION

App

NETUNNELPROVIDER MANAGER

Extension

NEPACKETTUNNEL PROVIDER

NEAPPPROXYPROVIDER

TUNNEL PROVIDER MANAGER

- Tunnel配置读取，开启连接
- 连接状态监控

PACKET TUNNEL PROVIDER

- IP layer tunneling
- tunnel网络配置（proxy, routes, exception list）

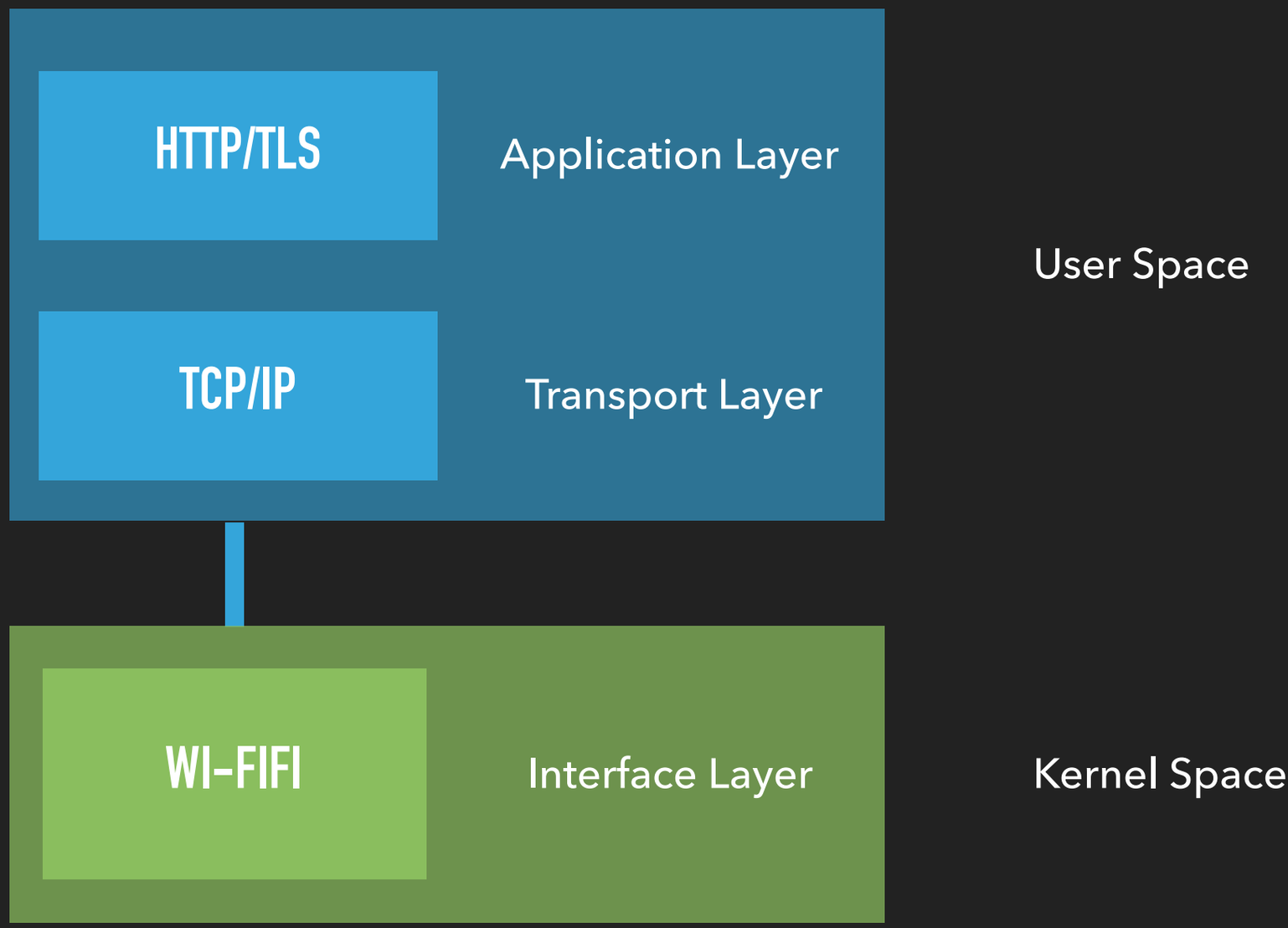
PACKET TUNNEL FLOW

- packets read/write

WWDC 2017

ADVANCES IN NETWORKING

Network Stack Evolution



NETWORK STACK EVOLUTION

- TCP/IP协议栈在内核态，协议处理在用户态；数据处理需要上下文切换。
- iOS 11中协议栈迁移到用户态，网络调度更加合理。
- 由Network Kernel Extension到Network Extension

AGENDA

- 概览
- NE介绍
- 基于NE的流量分析

基于NE的流量分析

- Surge/Potatso

在扩展里实现Proxy会怎样

App

NETUNNELPROVIDER

DASHBOARD

Extension

NEPACKETTUNNEL PROVIDER

STATISTICS MANAGER

bypass

bypass

HTTP PROXY

TCP PROXY

DEFAULT

HTTP PROXY

- 维护Tunnel集合
- HTTP Header解析
- Chunked处理
- User Agent

TCP PROXY

- 用户态的TCP/IP Stack
- DNS query
- lwip

THANKS